Yee & Associates, P.C.

13760 Noel Road
Suite 900
Dallas, Texas 75240

Main No. (972) 367-2001
Facsimile (972) 367-2008

Facsimile Cover Sheet

To: Commissioner for Patents for **Examiner Tran, Ellen C.** **Group Art Unit 2134**	Facsimile No.: **703/872-9306**
From: Monica Gamez Legal Assistant to Ted Fay	No. of Pages Including Cover Sheet: **34**
Message: Enclosed herewith: • Transmittal Document; and • Appeal Brief.	
Re: Application No. **09/503,608** Attorney Docket No: **RSW00-0010**	
Date: Wednesday, October 20, 2004	
Please contact us at (972) 367-2001 if you do not receive all pages indicated above or experience any difficulty in receiving this facsimile.	*This Facsimile is intended only for the use of the addressee and, if the addressee is a client or their agent, contains privileged and confidential information. If you are not the intended recipient of this facsimile, you have received this facsimile inadvertently and in error. Any review, dissemination, distribution, or copying is strictly prohibited. If you received this facsimile in error, please notify us by telephone and return the facsimile to us immediately.*

PLEASE CONFIRM RECEIPT OF THIS TRANSMISSION BY FAXING A CONFIRMATION TO 972-367-2008.

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of: **Attwood et al.**

Serial No.: **09/503,608**

Filed: **February 11, 2000**

For: **Technique of Defending Against Network Flooding Attacks Using a Connectionless Protocol**

Group Art Unit: **2134**

Examiner: **Tran, Ellen C.**

Attorney Docket No.: **RSW00-0010**

36736
PATENT TRADEMARK OFFICE
CUSTOMER NUMBER

Certificate of Transmission Under 37 C.F.R. § 1.8(a)
I hereby certify this correspondence is being transmitted via facsimile to the Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450, facsimile number (703) 872-9306 on 10.20.04.

By: Monica Gamez
Monica Gamez

TRANSMITTAL DOCUMENT

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:
ENCLOSED HEREWITH:

- Appeal Brief (37 C.F.R. 41.37).

A fee of $340.00 is required for filing an Appellant's Brief. Please charge this fee to IBM Corporation Deposit Account No. 09-0461. No additional fees are believed to be necessary. If, however, any additional fees are required, I authorize the Commissioner to charge these fees which may be required to IBM Corporation Deposit Account No. 09-0461. No extension of time is believed to be necessary. If, however, an extension of time is required, the extension is requested, and I authorize the Commissioner to charge any fees for this extension to IBM Corporation Deposit Account No. 09-0461.

Respectfully submitted,

Duke W. Yee
Registration No. 34,285
YEE & ASSOCIATES, P.C.
P.O. Box 802333
Dallas, Texas 75380
(972) 367-2001
ATTORNEY FOR APPLICANTS

Docket No. RSW00-0010 ***PATENT***

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of: **Attwood et al.**
Serial No. **09/503,608**
Filed: **February 11, 2000**
For: **Technique of Defending Against Network Flooding Attacks Using a Connectionless Protocol**

Group Art Unit: **2134**
Examiner: **Tran, Ellen C.**

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

APPEAL BRIEF (37 C.F.R. § 41.37)

This brief is in furtherance of the Notice of Appeal, filed in this case on August 20, 2004.

The fees required under 37 C.F.R. § 41.20, and any required petition for extension of time for filing this brief and fees therefore, are dealt with in the accompanying TRANSMITTAL OF APPEAL BRIEF.

REAL PARTIES IN INTEREST

The real party in interest in this appeal is the following party: International Business Machines Corporation.

RELATED APPEALS AND INTERFERENCES

With respect to other appeals or interference's that will directly affect, or be directly affected by, or have a bearing on the Board's decision in the pending appeal, there are no such appeals or interferences.

STATUS OF CLAIMS

A. TOTAL NUMBER OF CLAIMS IN APPLICATION

Claims in the application are: 1 through 14.

B. STATUS OF ALL THE CLAIMS IN APPLICATION

1. Claims canceled: None.
2. Claims withdrawn from consideration but not canceled: None.
3. Claims pending: 1 through 14.
4. Claims allowed: None.
5. Claims rejected: 1 through 14.

C. CLAIMS ON APPEAL

The claims on appeal are: 1 through 14.

STATUS OF AMENDMENTS

An amendment was filed after the final rejection of April 22, 2004. The advisory action of August 9, 2004 states that the amendment was not entered.

SUMMARY OF CLAIMED SUBJECT MATTER

A. CLAIMS 1, 5 and 7 - INDEPENDENT

Claim 1 is directed to a method of preventing a flood attack on a network server. Specification p. 1, ll. 7-10. A flooding attack on a network server includes sending an overwhelming number of datagrams to a server. Specification p. 1, l. 12 through p. 2, l. 2. The effect of the attack may cause the server to crash or to deny service to datagrams considered legitimate by the user of the server. Specification p. 2, ll. 2-8.

The claimed method addresses the problem of flooding attacks by determining how many datagrams are queued at a port on a network server and discarding queued datagrams when the number of queued datagrams exceeds a prescribed number. Specification p. 3, ll. 3-16. By analogy, the claimed method throws out legitimate datagrams along with illegitimate datagrams in order to preserve the server's capability of addressing some legitimate datagrams.

Specifically, the method determines, in response to a datagram received from a host for the port on the network server, whether the number of connectionless datagrams queued to a port on a server exceeds a prescribed threshold, discards the datagram if the number of datagrams already queued to the port exceeds the proscribed threshold and queues the datagram to a port on the server if the number of datagrams already queued to the port does not exceed the prescribed threshold. Specification p. 3, ll. 11-16; Figure 1.

Independent claims 5 and 7 contain the same patentable features. Claim 5 is directed to storage media containing program code for carrying out the method. Claim 7 is directed to a carrier wave containing programming code operable by the network server to carry out the method.

B. CLAIM 3 - INDEPENDENT

Claim 3 is directed to an apparatus for preventing a flood attack on a network server. Specification p. 1, ll. 7-10. The apparatus includes means for determining, in response to a

datagram from a host for the port on the network server, if the number of datagrams queued on the port by the host exceeds a prescribed threshold; means responsive to the determining means for discarding the datagram, if the number of datagrams queued on the port by the host exceeds the prescribed threshold; and means for queuing the datagram to a queue slot of the port, if the number of datagrams queued on the port by the host does not exceed the prescribed threshold. Specification p. 4, l. 21 through p. 7, l. 6. (The means includes a network server, which includes at least one processor, network communication software and at least one data port.)

C. CLAIM 4 – DEPENDENT ON CLAIM 3

Claim 4 further limits claim 3 by specifying that the means for determining further comprises means for calculating the prescribed threshold by multiplying a percentage P by a number of available queue slots for the port. Specification p. 6, ll. 14-26. (The means includes a network server, which includes at least one processor, network communication software and at least one data port.)

D. CLAIM 12 – DEPENDENT ON CLAIM 3

Claim 12 further limits claim 3 by including a means for configuring a maximum number of connectionless datagrams allowed to be queued at the port. Specification p. 4, l. 21 through p. 7, l. 6. (The means includes a network server, which includes at least one processor, network communication software and at least one data port.)

E. CLAIM 13 – DEPENDENT ON CLAIM 12

Claim 13 further limits claim 12 by specifying that the means for configuring further comprises a controlling percentage of available queue slots remaining for the port. Specification p. 6, ll. 14-26.

GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

A. GROUND OF REJECTION 1 (Claims 1 through 10 and 12 through 14)

Claims 1 through 10 and 12 through 14 stand rejected under 35 U.S.C. § 103(a) as obvious over Wesinger, Jr. et al., Firewall Providing Enhanced Network Security and User Transparency, U.S. Patent 6,052,788 (Apr. 18, 2000) in view of Reid, et al., System and Method for Controlling Interactions Between Networks, U.S. Patent 6,182,226 (Jan. 30, 2001).

B. GROUND OF REJECTION 2 (Claim 11)

Claim 11 stands rejected under 35 U.S.C. § 103(a) as obvious over Wesinger and Reid in view of Bechtolsheim, et al., Per-Flow Dynamic Buffer Management, U.S. Patent 6,515,963 (Feb. 4, 2003).

ARGUMENT

A. GROUND OF REJECTION 1 (Claims 1 through 10 and 12 through 14)

A.1. Claim 1

A.1.1. Technology Reflected in Claim 1

Claim 1 is directed to a method of preventing a flood attack on a network server. Specification p. 1, ll. 7-10. A flooding attack on a network server includes sending an overwhelming number of datagrams to a server. Specification p. 1, l. 12 through p. 2, l. 2. The effect of the attack may cause the server to crash or to deny service to datagrams considered legitimate by the user of the server. Specification p. 2, ll. 2-8. The claimed method addresses the problem of flooding attacks by determining how many datagrams are queued at a port on a network server and discarding queued datagrams when the number of queued datagrams exceeds a prescribed number. Specification p. 3, ll. 3-16. By analogy, the claimed method throws out the legitimate datagrams along with the illegitimate datagrams in order to preserve the server's capability of addressing some legitimate datagrams.

A.1.2. Summary of the Rejection

The thrust of the rejection of claim 1 is that Wesinger shows the claimed methods and devices, except for specifying that the disclosed methods and devices can be used to prevent flooding attacks, that Reid discusses preventing flooding attacks and that it would have been obvious to use Wesinger's methods and devices to prevent flooding attacks because Reid states that firewalls have become a key tool in controlling the flow of data in order to protect against malicious activities. However, the rejections are based a fundamentally flawed reading of Wesinger and on a flawed motivation to combine the references. As shown below, every statement the Examiner makes regarding what Wesinger teaches in relation to the claim language at issue is incorrect. Thus, the proposed combination does not result in the claimed inventions. In addition, the offered motivation is insufficient to sustain an obviousness rejection. Thus, the Examiner has failed to state

prima facie obviousness rejections. Furthermore, Wesinger teaches against the claims and no motivation exists to combine or modify the references in a way that would meet the claimed inventions. Therefore, claims 1 through 10 and 12 through 14 are non-obvious.

A.1.3. Standard for Obviousness Rejections

A proper prima facie case of obviousness must be supported by some teaching, suggestion or incentive supporting the combination. Obviousness cannot be established by combining the teachings of the prior art to produce the claimed invention absent some teaching, suggestion or incentive supporting the combination. In re Geiger, 815 F.2d 686, 688, 2 U.S.P.Q.2d 1276, 1278 (Fed. Cir. 1987).

Applicants respectfully submit that the references cited cannot be combined to produce the claimed invention because neither Wesinger nor Reid give any teaching, suggestion, or incentive to perform any of the claimed steps or make any of the claimed devices. As shown below, the Examiner has not pointed out any teaching, suggestion, or incentive in the prior art to perform any of the claimed steps or make any of the claimed devices.

A.1.4. The Examiner Fails To Point Out Any Teaching, Suggestion or Incentive in the Prior Art to Perform Any of the Claimed Steps or Make Any of the Claimed Devices

A.1.4.1. The Examiner's First Characterization of Claim 1 in the Light of Wesinger is Incorrect

Regarding claim 1, the Examiner states that the claimed phrase, "in which a large number of connectionless datagrams are received for queuing to a port on the network server, comprising:" is shown in Wesinger, col. 3, ll. 55-64. The Examiner specifically quotes that, "Both connection-oriented (e.g. TCP) and connectionless (e.g. UDP-based) services may be handled using envoys."

The examiner's characterization that the quoted language in Wesinger discloses the claim language is incorrect. An envoy is a word used by Wesinger to mean "An intervening program that functions as a transparent applications gateway." Wesinger, col. 5, ll. 37-38. Thus, an envoy is like a proxy server, which is a program or computer that emulates the main server in order to protect the main server from attack. Wesinger's envoy system, by his own description, is a firewall. Wesinger, col. 6, ll. 12-13. A firewall exists outside a server and prevents illegitimate datagrams from entering a port on a server in the first place. In contrast, the claimed method deals with managing datagrams that actually reach a port on the server. Although Wesinger claims that his "envoys" can handle connectionless services (connectionless datagrams), Wesinger does not show or suggest the process of managing connectionless datagrams queuing at a server port. Instead, one of ordinary skill would understand that Wesinger's firewall identifies illegitimate datagrams before they reach the server; thus, the text cited by the Examiner does not disclose the claim language at issue. In addition, Wesinger never discloses managing datagrams queued at a port on a server. Reid fails to cure the lack of disclosure in Wesinger. Thus, the proposed combination does not result in the claimed invention.

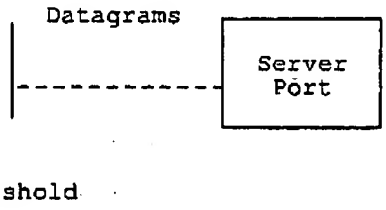
A.1.4.2. The Examiner's Second Characterization of Claim 1 in the Light of Wesinger is Incorrect

The Examiner then states that the claimed phrase, "determining, in response to the arrival of a connectionless datagram from a host for a port on the network server, if the number of connectionless datagrams already queued to the port from the host exceeds a prescribed threshold" is shown in Wesinger, col. 14, ll. 22-31. The Examiner specifically quotes:

> The firewall is capable of servicing many simultaneous connections. The number of allowable simultaneous connections is configurable and may be limited to a predetermined number, or may be limited not by number but only by the load currently experienced by the physical machine.

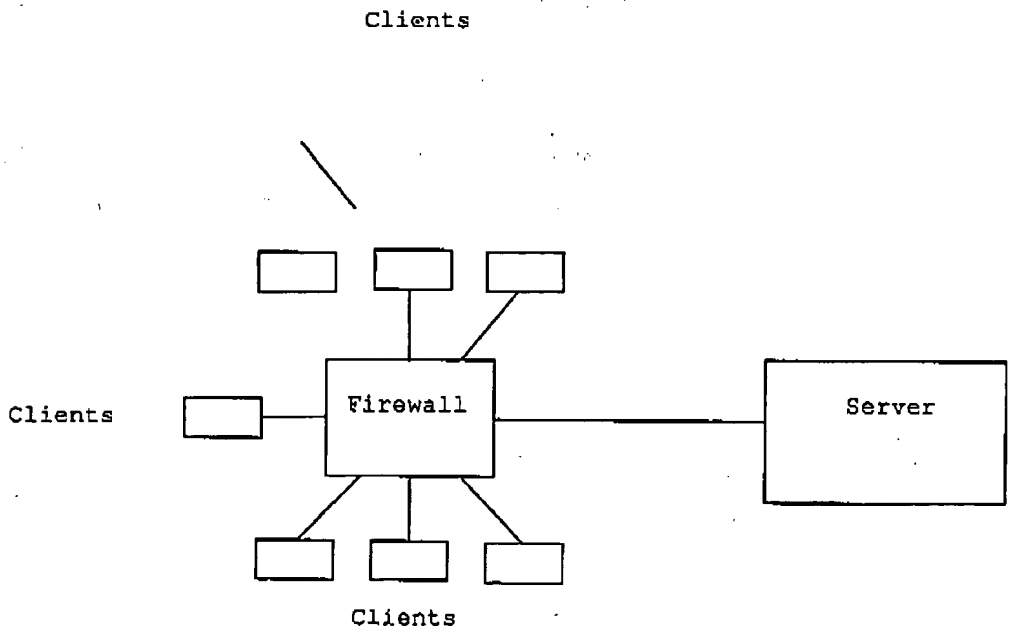
Wesinger, col. 14, ll. 22-27.

The examiner's characterization that the quoted language in Wesinger discloses the claim language is manifestly incorrect. The claim language at issue is directed towards determining if the number of datagrams already queued to a port exceeds a prescribed threshold. Thus, the method reflected by the claim language may be characterized by the following schematic, which shows a maximum number of datagrams queued at a port, where the maximum is set by the threshold:



(This schematic is a non-limiting example of how the claimed invention functions.)

On the other hand, the cited text in Wesinger describes the number of connections his firewall will allow to be made to the server. In other words, Wesinger is discussing how many client computers can simultaneously connect to the server through the firewall. Thus, Wesinger's disclosure may be characterized by the following schematic:



Wesinger merely limits the number of clients that *simultaneously* and *directly* connect through the firewall to the server, and is unconcerned with the number of *queued connectionless* datagrams at a server port. Given that each client connection is a direct connection (as opposed to dealing with the claimed connectionless datagrams), it is clear that Wesinger is utterly devoid of disclosure regarding the claimed inventions. Reid fails to cure the lack of disclosure in Wesinger in this regard. Accordingly, the proposed combination does not result in the claimed invention.

A.1.4.3. The Examiner's Characterization that Connectionless-Based Communications and Connection-Based Communications Can Be Addressed in the Same Manner Is Incorrect

Regarding the difference between connection-based and connectionless-based communications, in the Advisory Action of August 9, 2004, the Examiner states, "it is obvious in the art that 'connection' and 'connectionless' diagrams can be addressed in the same manner." The examiner points to the text book by R. Richard Stevens, TCP/IP Illustrated, and quotes as follows:

> IP is the workhouse protocol of the TCP/IP protocol suite. All TCP, UDP, ICMP and IGMP data gets transmitted as IP datagrams... A fact that amazes many newcomers to TCP/IP... is that IP provides an unreliable, connectionless datagram delivery service. The term connectionless means that IP does not maintain any state information about successive datagrams. Each datagram is handled independently from all other datagrams.

Advisory Action of August 9, 2004.

Again, the Examiner characterization of the reference is manifestly incorrect. On its face the text simply does not support the Examiner's assertion. Stevens describes how connectionless datagrams are created and transmitted and does not discuss direct connections in the cited text.

Anyone of ordinary skill in the art knows that direct connections are a reliable method of transmitting data because a direct connection is established between the server and the client. On

the other hand, when connectionless datagrams are used to send information from a client to a host, data is broken into packets that can take many different paths to reach the final destination. No direct connection exists between the client and the server. Each packet can travel through many routers or routing computers before arriving at its destination. Each packet is handled independently and can take different paths. After all the packets are received, the packets are then reassembled at the receiving computer. Because many paths can, and usually are taken, packets can become lost or corrupted. Thus, connectionless datagrams are said to be unreliable. Connectionless datagrams are controlled by TCP/IP (Transmission Control Protocol/ Internet Protocol). TCP deals with breaking the data into packets and reassembling them. IP deals with routing the data packets to the proper destination.

The fundamental difference between how connection-based and connectionless-based communication systems operate emphasizes the vast differences between the firewall described in the cited text in Wesinger, which handles direct connections in the text primarily cited by the Examiner, and the claimed method, which manages connectionless datagrams queuing at a server port. Thus, again, the proposed combination does not result in the claimed invention.

A.1.4.4. The Examiner's Third Characterization of Claim 1 in the Light of Wesinger is Incorrect

Returning to the rejection of claim 1, the Examiner then states that the claimed phrase, "discarding the datagram, if the number of connectionless datagrams already queued to the port from the host exceeds the prescribed threshold," is disclosed in Wesinger, col. 14, ll. 36-37. The cited text provides that, "the firewall selectively allows and denies connections to implement a network security policy."

The examiner's characterization that the quoted language in Wesinger discloses the claim language is manifestly incorrect. As shown above, Wesinger shows that his firewall allows or disallows *direct* connections between client computers and the server based on the identity of the clients. Even if Wesinger's firewall were handling connectionless datagrams, Wesinger would addresses managing the datagrams with the firewall before they reach the server. Wesinger is

devoid of disclosure regarding discarding datagrams once they actually reach the server port. Reid fails to cure the lack of disclosure in Wesinger in this regard. Accordingly, the proposed combination does not result in the claimed inventions.

A.1.4.5. The Examiner's Fourth Characterization of Claim 1 in the Light of Wesinger is Incorrect

The Examiner then states that the claimed phrase, "queuing the connectionless datagram to a queue slot of the port, if the number of connectionless datagrams already queued to the port from the host does not exceed the prescribed threshold is disclosed in Wesinger, col. 7, ll. 1-4. The cited text provides that, "The connection, once established, is fully bi-directional, with the same virtual host passing data between the originating network connection and the network connection at the opposite edge of the firewall."

The examiner's characterization that the quoted language in Wesinger discloses the claim language is manifestly incorrect. Wesinger describes bi-directional, direct connection through the virtual host between the originating network connection and the network connection at the opposite edge of the *firewall*. See Wesinger col. 6, ll. 61-65 through col. 7, ll. 1-4; see also Wesinger Fig. 1. On the other hand, the claim language at issue describes queuing a connectionless datagram to a queue slot *on a server port* if the number of datagrams already queued do not exceed the prescribed threshold. The claimed method of queuing connectionless datagrams at a server port is alien to Wesinger's method of establishing direct connections within a firewall. Reid fails to cure the lack of disclosure in Wesinger in this regard. Accordingly, the proposed combination fails to result in the claimed inventions.

A.1.4.6. The Examiner's Failure to Logically Connect the Cited Reference to Claim 1 Mandates that the Proposed Combination Does Not Result in the Claimed Invention

The failure of the Examiner to logically connect the cited text to any of the language of claim 1 belies the Examiner's fundamental misunderstanding of both Wesinger and the claimed

technology. Claim 1 is directed to a method of queuing and discarding connectionless datagrams received at a port on a server. Wesinger shows a modified proxy-type firewall, which prevents unauthorized connections (or unauthorized datagrams) from reaching a server in the first place. In addition, the method of claim 1 discards datagrams regardless of whether the datagrams are authorized or not. Firewalls, including the one shown in Wesinger, attempt to identify incoming connections or incoming datagrams and deny access to connections (or datagrams) that do not meet certain identification criteria. Although Wesinger does show that the number of direct connections to the firewall may be limited, Wesinger is silent regarding handling datagrams that ultimately reach a port on a server. Thus, even if the Wesinger firewall was somehow modified to protect against flooding attacks, it would do so in a completely different manner than the claimed method. Reid also only deals with firewalls. Although Reid does mention the term "flooding attack," Reid does not cure the lack of disclosure in Wesinger in this regard. Because none of the claim limitations are shown in either Wesinger or Reid, the proposed combination does not result in the invention of claim 1.

A.1.4.7. An Inherent Weakness in the Cited Art Emphasizes that the Proposed Combination Does Not Result in the Claimed Invention

The difference between the method of the proposed combination and the claimed method is emphasized by an inherent weakness in the method of the proposed combination. Perpetrators of malicious flooding attacks often forge the identity of the client computer from which a flooding attack is sent. Thus, datagrams sent from a client computer can "appear" to originate from an authorized client. In other words, the datagrams have a forged identify and may be considered forged datagrams. When a server protected by the Wesinger firewall is attacked by a flood of forged datagrams, the firewall will allow the flood of data to pass through the firewall because the firewall believes that all of the forged datagrams are authorized. Accordingly, the server would be overwhelmed despite the presence of the Wesinger firewall. On the other hand, the claimed method discards both authorized and unauthorized datagrams if the total number of queued datagrams exceeds the claimed threshold. Thus, a server protected by the claimed method will not be overwhelmed even if subject to a severe flooding attack of forged datagrams. (By analogy, the claimed method "throws out the good with the bad" whereas Wesinger, Reid and other firewalls

attempt to "separate the good from the bad.") The difference between the method of claim 1 and the method of the proposed combination emphasizes that Wesinger cannot disclose the claimed method. Similarly, Reid shows a firewall and suffers from the same weakness. Because Reid does not cure the lack of disclosure in Wesinger, the proposed combination does not result in the claimed inventions.

Because the Examiner has not pointed out any teaching, suggestion, or incentive in the cited references to perform any of the claimed steps or make any of the claimed devices, the Examiner has failed to state a prima facie obviousness rejection. Accordingly, Applicants respectfully request that the rejection be overturned and the claims allowed.

A.1.5 No Motivation Exists to Combine the References

A.1.5.1. A Pre-Existing Motivation to Combine the References Must Exist in Order To Establish a Prima Facie Obviousness Rejection

The mere fact that the prior art could be readily modified to arrive at the claimed invention does not render the claimed invention obvious; the prior art must suggest the desirability of such a modification. *In re Ochiai*, 71 F.3d 1565, 1570, 37 U.S.P.Q.2d 1127, 1131 (Fed. Cir. 1996); *In re Gordon*, 733 F.2d 900, 903, 221 U.S.P.Q. 1125, 1127 (Fed. Cir. 1984). Merely stating that the modification would have been obvious to one of ordinary skill without identifying an incentive or motivation for making the proposed modification is insufficient to establish a *prima facie* case.

A.1.5.2. No Motivation Exists To Combine the Cited Art

The complete lack of disclosure in Wesinger and Reid regarding the claimed method shows that the claimed method is utterly unsuggested in the known references. Furthermore, the claimed method is not suggested in the art. Thus, it is not possible to create a motivation to combine the references in a way that meets the claimed invention. Accordingly, the claims are non-obvious in view of Wesinger and Reid.

A.1.5.3. The Examiner Has Failed to Provide a Motivation To Combine the Cited Art

Further regarding a motivation to combine the references, the Examiner contends that the proposed combination is obvious because it would be obvious to modify a firewall to protect against flooding attacks. The statement makes no sense because firewalls prevent unauthorized connections or unauthorized datagrams from reaching the server in the first place. Thus, firewalls already defend against flooding attacks, though in a manner distinct from the claimed method. Accordingly, it makes no sense to state that it would be obvious to modify firewalls to protect against flooding attacks.

The Examiner attempts to bolster the assertion by quoting that, "firewalls have become a key tool in controlling the flow of data" and that users experience "increased vulnerability to malicious activities." These facts might motivate one to modify existing firewalls in a manner suggested by the prior art. However, the mere existence of a serious problem cannot motivate one of only ordinary skill to completely depart from the prior art and propose an otherwise unsuggested solution (especially when the solution calls for discarding authorized datagrams along with the unauthorized datagrams.) Thus, the Examiner failed to provide a motivation to combine the references. Accordingly, the Examiner failed to state a prima facie obviousness rejection of claim 1.

A.1.6 Wesinger Teaches Away from Claim 1

For similar reasons, Wesinger teaches away from claim 1. Wesinger, like most firewall devices, teaches that incoming datagrams and direct connections should be identified so that authorized datagrams and authorized connections may be allowed through the firewall and unauthorized datagrams and unauthorized connections may be excluded from the firewall. See Wesinger col. 3, ll. 60-62, "No traffic can pass through the firewall unless the firewall has established an envoy for that traffic." (The envoy establishes a transparent proxy for the server.) See also col. 1, ll. 12-17, "The present invention relates to computer network security and more particularly to firewalls, i.e., a combination of computer hardware and software that selectively allows 'acceptable' computer transmissions to pass through it and disallows other non-acceptable

computer transmissions." One of ordinary skill, upon reading Wesinger, might be motivated to create a device that selectively allows "authorized" datagrams to pass to a server. Wesinger would motivate one of ordinary skill to avoid discarding both authorized and unauthorized datagrams because doing so defeats the purpose of a firewall, which is to identify and allow authorized transmissions. Because Wesinger teaches away from claim 1, claim 1 is non-obvious.

A.2. Claim 2

Regarding claim 2, the proposed combination does not result in the claimed invention. The Examiner contends that Wesinger discloses the claimed step of calculating the prescribed threshold by multiplying a percentage P by the number of available queue slots for the port. The Examiner points to Wesinger, col. 14, ll. 22-31, which describes that the number of connections to the firewall may be limited. As pointed out with the above schematic drawings, Wesinger does not disclose managing datagrams at a server port as claimed, but rather discloses limiting direct connections between client computers and a firewall. Wesinger is devoid of disclosure regarding the subject matter of claim 2 and Reid fails to cure the lack of disclosure in Wesinger. Thus, the proposed combination does not result in the claimed invention. For similar reasons, claim 2 is independently patentable over the proposed combination.

A.3. Claim 3

Regarding claim 3, the proposed combination does not result in the claimed invention. The Examiner contends that claim 3 is directed to the apparatus of the method of claim 1 and is rejected under the same rationale. As pointed out with the above schematic drawings, Wesinger does not disclose a device for managing datagrams at a server port as claimed, but rather discloses limiting direct connections between client computers and a firewall. Wesinger is devoid of disclosure regarding the subject matter of claim 3 (apparatus for preventing a flood attack, including means for queuing a datagram to a queue slot of a server port if the number of datagrams queued on the port by the host does not exceed a prescribed threshold) and Reid fails to cure the lack of disclosure in Wesinger. Thus, the proposed combination does not result in the claimed invention. For similar reasons, claim 3 is independently patentable over the proposed combination.

A.4. Claim 4

Regarding claim 4, the proposed combination does not result in the claimed invention. The Examiner contends that claim 4 is directed to similar subject matter of the apparatus of claim 1 and is rejected under the same rationale. As pointed out with the above schematic drawings, Wesinger does not disclose a device for managing datagrams at a server port as claimed, but rather discloses limiting direct connections between client computers and a firewall. Wesinger is devoid of disclosure regarding the subject matter of claim 4 (means for calculating the prescribed threshold by multiplying a percentage P by a number of available queue slots for the port) and Reid fails to cure the lack of disclosure in Wesinger. Thus, the proposed combination does not result in the claimed invention. For similar reasons, claim 4 is independently patentable over the proposed combination.

A.5 Claim 5

Regarding claim 5, the proposed combination does not result in the claimed invention. The Examiner contends that claim 5 is directed to storage media containing program code of the method of claim 1 and is rejected under the same rationale. As pointed out with the above schematic drawings, Wesinger does not disclose a device for managing datagrams at a server port as claimed, but rather discloses limiting direct connections between client computers and a firewall. Wesinger is devoid of disclosure regarding the subject matter of claim 5 (storage media containing code to perform a method similar to claim 1) and Reid fails to cure the lack of disclosure in Wesinger. Thus, the proposed combination does not result in the claimed invention. For similar reasons, claim 5 is independently patentable over the proposed combination.

A.6. Claim 6

Regarding claim 6, the proposed combination does not result in the claimed invention. The Examiner contends that claim 6 incorporates substantially similar subject matter as recited in claim 2 and is rejected under the same rationale. As pointed out with the above schematic drawings, Wesinger does not disclose a device for managing datagrams at a server port as claimed, but rather discloses limiting direct connections between client computers and a firewall. Wesinger is devoid

of disclosure regarding the subject matter of claim 6 (storage media containing code for calculating the prescribed threshold by multiplying a percentage P by a number of available queue slots for the port) and Reid fails to cure the lack of disclosure in Wesinger. Thus, the proposed combination does not result in the claimed invention. For similar reasons, claim 6 is independently patentable over the proposed combination.

A.7. Claim 7

Regarding claim 7, the proposed combination does not result in the claimed invention. The Examiner contends that claim 7 is directed to a carrier wave containing program code of the method of claim 1 and is rejected under the same rationale. As pointed out with the above schematic drawings, Wesinger does not disclose a device for managing datagrams at a server port as claimed, but rather discloses limiting direct connections between client computers and a firewall. Wesinger is devoid of disclosure regarding the subject matter of claim 7 (a carrier wave containing program code for performing steps similar to claim 1) and Reid fails to cure the lack of disclosure in Wesinger. Thus, the proposed combination does not result in the claimed invention. For similar reasons, claim 7 is independently patentable over the proposed combination.

A.8. Claim 8

Regarding claim 8, the proposed combination does not result in the claimed invention. The Examiner contends that claim 8 incorporates substantially similar subject matter as in claim 2 and is rejected under the same rationale. As pointed out with the above schematic drawings, Wesinger does not disclose a device for managing datagrams at a server port as claimed, but rather discloses limiting direct connections between client computers and a firewall. Wesinger is devoid of disclosure regarding the subject matter of claim 8 (a carrier wave containing code for calculating the prescribed threshold by multiplying a percentage P by a number of available queue slots for the port) and Reid fails to cure the lack of disclosure in Wesinger. Thus, the proposed combination does not result in the claimed invention. For similar reasons, claim 8 is independently patentable over the proposed combination.

A.9. Claim 9

Regarding claim 9, the proposed combination does not result in the claimed invention. The Examiner contends that the claimed phrase, "...configuring a maximum number of connectionless datagrams allowed to be queued at the port" is taught by Wesinger in col. 14, ll. 22-31, which provides that the firewall is capable of serving many simultaneous connections. As pointed out with the above schematic drawings, Wesinger does not disclose a device for managing datagrams at a server port as claimed, but rather discloses limiting direct connections between client computers and a firewall. Wesinger is devoid of disclosure regarding the subject matter of claim 9 (configuring a maximum number of connectionless datagrams allowed to be queued at the port) and Reid fails to cure the lack of disclosure in Wesinger. Thus, the proposed combination does not result in the claimed invention. For similar reasons, claim 9 is independently patentable over the proposed combination.

A.10 Claim 10

Regarding claim 10, the proposed combination does not result in the claimed invention. The Examiner points to the same text in Wesinger (col. 14, ll. 22-31) to support the rejection. As pointed out with the above schematic drawings, Wesinger does not disclose a device for managing datagrams at a server port as claimed, but rather discloses limiting direct connections between client computers and a firewall. Wesinger is devoid of disclosure regarding the subject matter of claim 10 (wherein the prescribed threshold of claim 9 is based on the controlling percentage of available queue slots remaining for the port) and Reid fails to cure the lack of disclosure in Wesinger. Thus, the proposed combination does not result in the claimed invention. For similar reasons, claim 10 is independently patentable over the proposed combination.

A.11 Claim 12

Regarding claim 12, the proposed combination does not result in the claimed invention. The Examiner contends that claim 12 incorporates substantially similar subject matter as in claim 9 and is rejected under the same rationale. As pointed out with the above schematic drawings,

Wesinger does not disclose a device for managing datagrams at a server port as claimed, but rather discloses limiting direct connections between client computers and a firewall. Wesinger is devoid of disclosure regarding the subject matter of claim 12 (means for configuring a maximum number of connectionless datagrams allowed to be queued at the port) and Reid fails to cure the lack of disclosure in Wesinger. Thus, the proposed combination does not result in the claimed invention. For similar reasons, claim 12 is independently patentable over the proposed combination.

A.12 Claim 13

Regarding claim 13, the proposed combination does not result in the claimed invention. The Examiner contends that claim 13 incorporates substantially similar subject matter as in claim 10 and is rejected under the same rationale. As pointed out with the above schematic drawings, Wesinger does not disclose a device for managing datagrams at a server port as claimed, but rather discloses limiting direct connections between client computers and a firewall. Wesinger is devoid of disclosure regarding the subject matter of claim 13 (the means for configuring further comprises configuring a controlling percentage of available queue slots remaining for the port) and Reid fails to cure the lack of disclosure in Wesinger. Thus, the proposed combination does not result in the claimed invention. For similar reasons, claim 13 is independently patentable over the proposed combination.

A.13 Claim 14

Regarding claim 13, the proposed combination does not result in the claimed invention. The Examiner contends that the claimed phrase, "wherein the computer is the network server" is taught in Reid, col. 3, ll. 1-8 and specifically quotes, "workstations 40 communicate through firewall 34 with servers or workstations on external network 36 and with server 42 on network 44." As pointed out with the above schematic drawings, Wesinger does not disclose a device for managing datagrams at a server port as claimed, but rather discloses limiting direct connections between client computers and a firewall. Reid fails to cure the lack of disclosure in Wesinger and the fact that Reid discloses the term "network server" is irrelevant to the underlying patentability of claim 14. Thus, the proposed combination does not result in the claimed invention. For similar

reasons, claim 14 is independently patentable over the proposed combination.

B. GROUND OF REJECTION 2 (Claim 11)

The rejection of claim 11 relies on the combination of Wesinger (U.S. Patent 6,052,788), Reid (U.S. Patent 6,182,226) and Bechtolsheim (U.S. Patent 6,515,963). The rejection rests on the Examiner's characterization of Wesinger, which as pointed out with respect to claim 1 is fundamentally flawed. The combination of Wesinger and Reid cannot show the limitations of independent claim 1, upon which claim 11 depends. In addition, Bechtolsheim shows a dynamic buffer management scheme, wherein the header information for each packet is mapped into an entry in a flow table. Data packets are enqueued in or dropped from a buffer based on the header information. Bechtolsheim is cumulative to Wesinger in the sense that data packets are identified and sorted according to information in the packet. Thus, Bechtolsheim does not cure the lack of disclosure in Wesinger. Because none of the references show or suggest the claimed invention, it is not possible to show a teaching, suggestion or incentive supporting the combination under the standards of In re Geiger. Accordingly, Obviousness cannot be established.

In addition, the Examiner states that it would have been obvious to combine the references to include a means to maintain queue slots available in a port. The proposed motivation to make the modification is "to compensate for the different types of internetworking traffic or flows presented to the router/switching device... Buffer manager 25 and port scheduler 50 are also implemented."

However, the proposed motivation is irrelevant to claim 11. Claim 11 is directed to the method of claim 1 wherein the a port comprises a plurality of queue slots and the method further comprises maintaining a number of available queue slots of the plurality of queue slots for the port. The fact that Bechtolsheim discusses compensating for different *types* of networking traffic or flow is irrelevant to maintaining a number of available of queue slots in a plurality of queue slots. Thus, the Examiner has failed to provide a motivation to combine the references. Accordingly, the Examiner has failed to state a prima facie obviousness rejection of claim 11.

Furthermore, no motivation exists to combine the references to meet the limitations of claim 11. Claim 11 is directed to managing connectionless datagrams queued at a port on a server. All three references are devoid of disclosure in this regard. Because the references and the art fail suggest the claimed method, no motivation can exist to combine the references. Accordingly, claim 11 is non-obvious over the cited references.

CONCLUSION

The claimed methods and devices are directed to managing connectionless datagrams queued at a port on a server, wherein additional datagrams are discarded when the number of queued datagrams exceeds a prescribed limit. Thus, the claimed methods and devices discard both legitimate and illegitimate datagrams. On the other hand, Wesinger and Reid are directed towards firewalls, which seek to prevent illegitimate datagrams from reaching the server in the first place. The methods and devices shown in Wesinger and Reid are completely distinct from the claimed methods and devices and neither reference shows the limitations of the claims. In addition, Bechtolsheim is cumulative to Wesinger for purposes of the rejection of claim 11. Thus, the proposed combinations cannot result in the claimed inventions. Furthermore, Wesinger and Reid teach away from the claims and no motivation exists to combine the references. Thus, the claims are also non-obvious.

Applicants preserve all arguments made in the responses to the previous Office Actions.

Theodore D. Fay III
Reg. No. 48,504
YEE & ASSOCIATES, P.C.
PO Box 802333
Dallas, TX 75380
(972) 367-2001

APPENDIX OF CLAIMS

The claims involved in the appeal are:

1. (previously presented) A method of preventing a flooding attack on a network server in which a large number of connectionless datagrams are received for queuing to a port on the network server, comprising:

determining, in response to the arrival of a connectionless datagram from a host for a port on the network server, if the number of connectionless datagrams already queued to the port from the host exceeds a prescribed threshold;

discarding the datagram, if the number of connectionless datagram already queued to the port from the host exceeds the prescribed threshold; and

queuing the connectionless datagram to a queue slot of the port, if the number of connectionless datagram already queued to the port from the host does not exceed the prescribed threshold.

2. (previously presented) The method of claim 1 wherein the determining if the number of datagrams already queued to the port from the host exceeds a prescribed threshold further comprises:

calculating the prescribed threshold by multiplying a percentage P by the number of available queue slots for the port.

3. (previously presented) Apparatus for preventing a flooding attack on a network server in which a large number of datagrams are received for queuing to a port on the server, comprising:

means for determining, in response to a datagram from a host for the port on the network

server, if the number of datagrams queued on the port by the host exceeds a prescribed threshold; means responsive to the determining means for discarding the datagram, if the number of datagrams queued on the port by the host exceeds the prescribed threshold; and

means for queuing the datagram to a queue slot of the port, if the number of datagrams queued on the port by the host does not exceed the prescribed threshold.

4. (previously presented) The apparatus of claim 3 wherein the means for determining if the number of datagrams already queued to the port from the host exceeds a prescribed threshold further comprises:

means for calculating the prescribed threshold by multiplying a percentage P by a number of available queue slots for the port.

5. (previously presented) A storage media containing program code that is operable by a computer for preventing a flooding attack on a network server in which a large number of datagrams are received for queuing to a port on the network server, the program code including instructions for causing the computer to execute the steps of:

determining if the number of datagrams already queued to the port from the host exceeds a prescribed threshold, in response to a datagram from a host for the port on the network server;

discarding the datagram, if the number of datagrams already queued to the port from the S host exceeds the prescribed threshold; and

queuing the datagram to a queue slot of the port, if the number of datagrams already queued to the port from the S host does not exceed the prescribed threshold.

6. (previously presented) The storage media of claim 5 further comprising the step of:

calculating the prescribed threshold by multiplying a percentage P by a number of available queue slots for the port.

7. (previously presented) A carrier wave containing program code that is operable by a network server for preventing a flooding attack on the network server in which a large number of datagrams are received for queuing to a port on the server, the program code including instructions for causing the network server to execute the steps of:

determining, in response to receipt of a datagram from the host for queuing to the port on the network server, if the number of datagrams already queued to the port from a host exceeds a prescribed threshold;

discarding the datagram, if the number of datagrams already queued to the port from the host exceeds the prescribed threshold; and

queueing the datagram to the port, if the number of datagrams already queued to the port from the host does not exceed the prescribed threshold.

8. (previously presented) The carrier wave of claim 7 wherein the program code further includes instructions for causing the network server to execute the step of:

calculating the prescribed threshold by multiplying a percentage P by a number of available queue slots for the port.

9. (previously presented) The method of claim 1 further comprising:

configuring a maximum number of connectionless datagrams allowed to be queued at the port.

10. (previously presented) The method of claim 9 wherein the configuring step further includes configuring a controlling percentage of available queue slots remaining for the port; and

wherein the prescribed threshold is based on the controlling percentage of available queue slots remaining for the port.

11. (previously presented) The method of claim 1 wherein the port comprises a plurality of queue slots, the method further comprising:

maintaining a number of available queue slots of the plurality of queue slots for the port.

12. (previously presented) The apparatus of claim 3 further comprising:

a means for configuring a maximum number of connectionless datagrams allowed to be queued at the port.

13. (previously presented) The apparatus of claim 12 wherein the means for configuring further comprises configuring a controlling percentage of available queue slots remaining for the port.

14. (previously presented) The storage media of claim 5 wherein the computer is the network server.

EVIDENCE APPENDIX

There is no evidence to be presented.

RELATED PROCEEDINGS APPENDIX

There are no related proceedings.